PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-006608
(43)Date of publication of application : 10.01.1997

(51)Int.Cl. G06F 9/06
G06F 12/14

(21)Application number : 07-156538
(22)Date of filing : 22.06.1995

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MATSUZAKI NATSUME
OMORI MOTOJI
TATEBAYASHI MAKOTO

(54) SOFTWARE PROTECTION SYSTEM

(57)Abstract:

PURPOSE: To reduce the number or digits or data, especially, a random value on a communication line at the time of using the communication line to acquire the execution right of software.

CONSTITUTION: A software executer 101 generates the executer ID and order information and sends them to an order manager 102 to order the software. The order manager 102 generates an execution right generation password, which is information dependent upon received order information and executer secret information corresponding to the executer ID, and sends it to the software executer 101. The software executer 101 discriminates whether this execution right generation password matches with order information sent to the order manager 102 before and its own executer secret information or not; and if it matches, the software executer 101 generates the execution right of software corresponding to order information to execute this software.

LEGAL STATUS

[Date of request for examination] 29.06.2000

[Date of sending the examiner's

decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3570781

[Date of registration] 02.07.2004

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] It connects with one or more software effectors which perform offered software, and each software effector through a communication path. It is the software protection system equipped with the order management machine which manages the order of software received from each software effector. And each aforementioned software effector An effector ID storing means to store the effector ID of a proper, and the 1st confidential information storing means which stores the effector confidential information of a proper, The order creation means which creates the ordering information of the right of activation of one or more software, and carries out are recording maintenance is included. Said effector ID and said ordering information It is sent to said order management machine through said channel. Said order management machine The 2nd confidential information storing means which stores all the effector confidential information stored in each aforementioned software effector, The effector confidential information corresponding to the effector ID received from said software effector is gained from said 2nd confidential information storing means. A right generation password generation means of activation to generate the right generation password of activation depending on the ordering information received from this effector confidential information and software effector that were gained

is included. Said right generation password of activation is sent to said software effector through said channel. Each aforementioned software effector Furthermore, the ordering information by which are recording maintenance was carried out, and the effector confidential information stored in said 1st confidential information storing means are used for said order creation means. When the justification of said right generation password of activation is checked as a result of inspection by right generation password verification means of activation to inspect the justification of the right generation password of activation received from said order management machine, and said right generation password verification means of activation A software protection system including a right generation means of activation to generate the right of activation of the software an order with said order creation means for was placed based on the ordering information by which are recording maintenance was carried out, and a software activation means to perform software with which said right of activation exists according to the execution condition shown in the right of activation concerned.

[Claim 2] The ordering information which received said right generation password generation means of activation from said software effector, The effector confidential information gained from said 2nd confidential information storing means is inputted into a data compression function with which an output is related to all the input bits. The output of this data compression function is outputted as said right generation password of activation. Said right generation password verification means of activation The ordering information by which are recording maintenance was carried out, and the effector confidential information stored for said 1st confidential information storing means for said order creation means When in agreement with the right generation password of activation which entered into the same data compression function as the data compression function used with said right generation password generation means of activation, and the output received from the order management machine, The software protection system according to claim 1 characterized by judging that the right generation password of activation concerned is just.

[Claim 3] Said order management machine includes further the 3rd confidential information storing means which stores the confidential information used for a public key signature method. Said right generation password generation means of activation The confidential information stored in said 3rd confidential information storing means, and the effector confidential information gained from said 2nd

confidential information storing means, It uses with the ordering information received from said software effector, and the right generation password of activation by which the digital signature was carried out with the public key signature method is generated. Said software effector A public information storing means to store the public information corresponding to the confidential information used for said public key signature method is included further. Said right generation password verification means of activation Using the public information stored in said public information storing means, the ordering information by which are recording maintenance was carried out at said order creation means, and the effector confidential information stored for said 1st confidential information storing means with the signature check method corresponding to said public key signature method The software protection system according to claim 1 characterized by inspecting the justification of the right generation password of activation received from said order management machine.

[Claim 4] It connects with one or more software effectors which perform offered software, and each software effector through a communication path. It is the software protection system equipped with the order management machine which manages the order of software received from each software effector. And each aforementioned software effector An effector ID storing means to store the effector ID of a proper, and the 1st confidential information storing means which stores the effector confidential information of a proper, The order creation means which creates the ordering information of the right of activation of one or more software, and carries out are recording maintenance, The change value generation means which generates the change value which changes whenever ordering information is created with said order creation means, and carries out are recording maintenance is included. Said effector ID, said ordering information, and said change value It is sent to said order management machine through said channel. Said order management machine The 2nd confidential information storing means which stores all the effector confidential information stored in each aforementioned software effector, The effector confidential information corresponding to the effector ID received from said software effector is gained from said 2nd confidential information storing means. A right generation password generation means of activation to generate the right generation password of activation depending on this gained effector confidential information, the ordering information received from the software effector, and a change value is included. Said right generation password of activation is sent to said software effector through said channel.

Each aforementioned software effector The ordering information by which are recording maintenance was furthermore carried out at said order creation means, and the change value by which are recording maintenance was carried out at said change value generation means, A right generation password verification means of activation to inspect the justification of the right generation password of activation received from said order management machine using the effector confidential information stored in said 1st confidential information storing means, When the justification of said right generation password of activation is checked as a result of inspection by said right generation password verification means of activation A software protection system including a right generation means of activation to generate the right of activation of the software an order with said order creation means for was placed based on the ordering information by which are recording maintenance was carried out, and a software activation means to perform software with which said right of activation exists according to the execution condition shown in the right of activation concerned.

[Claim 5] The ordering information which received said right generation password generation means of activation from said software effector, and a change value, The effector confidential information gained from said 2nd confidential information storing means is inputted into a data compression function with which an output is related to all the input bits. The output of this data compression function is outputted as said right generation password of activation. Said right generation password verification means of activation The ordering information by which are recording maintenance was carried out at said order creation means, and the change value by which are recording maintenance was carried out at said change value generation means, The effector confidential information stored in said 1st confidential information storing means is inputted into the same data compression function as the data compression function used with said right generation password generation means of activation. The software protection system according to claim 4 characterized by judging that the right generation password of activation concerned is just when the output is in agreement with the right generation password of activation received from the order management machine.

[Claim 6] It connects with one or more software effectors which perform offered software, and each software effector through a communication path. It is the software protection system equipped with the order management machine which manages the order of software received from each software effector. And each aforementioned software effector An

effector ID storing means to store the effector ID of a proper, and the 1st confidential information storing means which stores the effector confidential information of a proper, The order creation means which creates the ordering information of the right of activation of one or more software, and carries out are recording maintenance, The 1st time stump generation means which generates a time stump and carries out are recording maintenance whenever ordering information is created with said order creation means is included. Said effector ID and said ordering information It is sent to said order management machine through said channel. Said order management machine The 2nd time stump generation means which will generate a time stump if Effector ID and ordering information are received from said software effector, The 2nd confidential information storing means which stores all the effector confidential information stored in each aforementioned software effector, The effector confidential information corresponding to the effector ID received from said software effector is gained from said 2nd confidential information storing means. This gained effector confidential information, A right generation password generation means of activation to generate the right generation password of activation depending on the ordering information received from the software effector and the time stump generated with said 2nd time stump generation means is included. Said right generation password of activation is sent to said software effector through said channel. Each aforementioned software effector The ordering information by which are recording maintenance was furthermore carried out at said order creation means, and the time stump by which are recording maintenance was carried out at said 1st time stump generation means, A right generation password verification means of activation to inspect the justification of the right generation password of activation received from said order management machine using the effector confidential information stored in said 1st confidential information storing means, When the justification of said right generation password of activation is checked as a result of inspection by said right generation password verification means of activation A software protection system including a right generation means of activation to generate the right of activation of the software an order with said order creation means for was placed based on the ordering information by which are recording maintenance was carried out, and a software activation means to perform software with which said right of activation exists according to the execution condition shown in the right of activation concerned.

[Claim 7] It connects with one or more software effectors which perform

offered software, and each software effector through a communication path. It is the software protection system equipped with the order management machine which manages the order of software received from each software effector. And each aforementioned software effector An effector ID storing means to store the effector ID of a proper, and the 1st confidential information storing means which stores the effector confidential information of a proper, The order creation means which creates the ordering information of the right of activation of one or more software, and carries out are recording maintenance, The order authentication information generation means which generates the order authentication information depending on said ordering information and said effector confidential information, and carries out are recording maintenance is included. Said effector ID, said ordering information, and said order authentication information It is sent to said order management machine through said channel. Said order management machine The 2nd confidential information storing means which stores all the effector confidential information stored in each aforementioned software effector, The effector confidential information corresponding to the effector ID received from said software effector is gained from said 2nd confidential information storing means. This gained effector confidential information, the ordering information received from the software effector, and order authentication information are used. An effector authentication means to perform authentication of a software effector and ordering information, and to treat the order authentication information concerned as order identification information which identifies an order when this authentication result is just, Only when the authentication result in said effector authentication means is just, a right generation password generation means of activation to generate the right generation password of activation depending on said ordering information and said order identification information is included. Said right generation password of activation is sent to said software effector through said channel with said order identification information. Each aforementioned software effector Furthermore, the ordering information by which are recording maintenance was carried out, and the order authentication information by which are recording maintenance was carried out at said order authentication information generation means are used for said order creation means. When the justification of said right generation password of activation is checked as a result of inspection by right generation password verification means of activation to inspect the justification of the right generation password of activation received from said order management machine, and said right

generation password verification means of activation A software protection system including a right generation means of activation to generate the right of activation of the software an order with said order creation means for was placed based on the ordering information by which are recording maintenance was carried out, and a software activation means to perform software with which said right of activation exists according to the execution condition shown in the right of activation concerned.

[Claim 8] The ordering information by which said order authentication information generation means was created with said order creation means, The effector confidential information stored in said 1st confidential information storing means is inputted into a data compression function with which an output is related to all the input bits. The output of this data compression function is outputted as said order authentication information. Said effector authentication means The effector confidential information gained from said 2nd confidential information storing means, and the ordering information received from the software effector It inputs into the same data compression function as the data compression function used with said order authentication information generation means. When the output of this data compression function is in agreement with the order authentication information received from the software effector It attests that the software effector and ordering information which placed an order are just. Said right generation password generation means of activation The ordering information received from said software effector, and said order identification information It inputs into the same data compression function as the data compression function used with said order authentication information generation means. The output of this data compression function is outputted as said right generation password of activation. Said right generation password verification means of activation The ordering information by which are recording maintenance was carried out, and the order authentication information by which are recording maintenance was carried out at said order authentication information generation means for said order creation means When in agreement with the right generation password of activation which entered into the same data compression function as the data compression function used with said order authentication information generation means, and the output received from the order management machine, The software protection system according to claim 7 characterized by judging that the right generation password of activation concerned is just.

[Claim 9] It connects with one or more software effectors which perform

offered software, and each software effector through a communication path. It is the software protection system equipped with the order management machine which manages the order of software received from each software effector. And each aforementioned software effector An effector ID storing means to store the effector ID of a proper, and the 1st confidential information storing means which stores the effector confidential information of a proper, The order creation means which creates the ordering information of the right of activation of one or more software, and carries out are recording maintenance, The change value generation means which generates the change value which changes whenever ordering information is created with said order creation means, and has predetermined DS or semantics, and carries out are recording maintenance, By calculating the value depending on said ordering information and said effector confidential information, and changing said change value with this calculated value The order authentication information generation means which generates order authentication information and carries out are recording maintenance is included. Said effector ID, said ordering information, and said order authentication information It is sent to said order management machine through said channel. Said order management machine The 2nd confidential information storing means which stores all the effector confidential information stored in each aforementioned software effector, The effector confidential information corresponding to the effector ID received from said software effector is gained from said 2nd confidential information storing means. The inverse transformation means which calculates the value depending on this effector confidential information and ordering information from a software effector that were gained, and carries out inverse transformation of the order authentication information from a software effector using this value, An effector authentication means to attest that a software effector and ordering information are just when it has the DS or semantics as said change value of said inverse transformation means with the same output, Only when the authentication result in said effector authentication means is just, a right generation password generation means of activation to generate the right generation password of activation depending on said ordering information is included. Said right generation password of activation is sent to said software effector through said channel. Each aforementioned software effector Furthermore, the ordering information by which are recording maintenance was carried out, and the order authentication information by which are recording maintenance was carried out at said order authentication information generation means are used for said order

creation means. When the justification of said right generation password of activation is checked as a result of inspection by right generation password verification means of activation to inspect the justification of the right generation password of activation received from said order management machine, and said right generation password verification means of activation A software protection system including a right generation means of activation to generate the right of activation of the software an order with said order creation means for was placed based on the ordering information by which are recording maintenance was carried out, and a software activation means to perform software with which said right of activation exists according to the execution condition shown in the right of activation concerned.

[Claim 10] The ordering information by which said order authentication information generation means was created with said order creation means, The effector confidential information stored in said 1st confidential information storing means is inputted into a data compression function with which an output is related to each input bits of all. The exclusive OR of the output and said change value is outputted as order authentication information. Said inverse transformation means The ordering information from a software effector, and the effector confidential information gained from said 2nd confidential information storing means By inputting into the same data compression function as the data compression function used with said order authentication information generation means, and calculating the exclusive OR of the output and order authentication information from a software effector Inverse transformation of the order authentication information concerned is carried out. Said right generation password generation means of activation The ordering information received from said software effector, and said order identification information It inputs into the same data compression function as the data compression function used with said order authentication information generation means. The output of this data compression function is outputted as said right generation password of activation. Said right generation password verification means of activation The ordering information by which are recording maintenance was carried out, and the order authentication information by which are recording maintenance was carried out at said order authentication information generation means for said order creation means When in agreement with the right generation password of activation which entered into the same data compression function as the data compression function used with said order authentication information generation means, and the output received from the order management machine, The software

protection system according to claim 9 characterized by judging that the right generation password of activation concerned is just.
[Claim 11] Said right generation password generation means of activation is added to the ordering information received from the software effector. The right generation password of activation depending on the effector confidential information gained from said 2nd confidential information storing means is generated. Said right generation password verification means of activation The ordering information by which are recording maintenance was carried out, and the effector confidential information stored in said 1st confidential information storing means are used for said order creation means. The software protection system according to claim 7 or 9 characterized by inspecting the justification of the right generation password of activation received from said order management machine.
[Claim 12] Said order management machine includes further the 3rd confidential information storing means which stores the confidential information used for a public key signature method. Said right generation password generation means of activation The confidential information stored in said 3rd confidential information storing means, and the effector confidential information gained from said 2nd confidential information storing means, The right generation password of activation by which the digital signature was carried out with the public key signature method is generated using the ordering information and the order authentication information which were received from said software effector. Said software effector A public information storing means to store the public information corresponding to the confidential information used for said public key signature method is included further. Said right generation password verification means of activation The public information stored in said public information storing means, and the ordering information by which are recording maintenance was carried out at said order creation means, Using the order authentication information by which are recording maintenance was carried out, and the effector confidential information stored for said 1st confidential information storing means with the signature check method corresponding to said public key signature method for said order authentication information generation means The software protection system according to claim 7 or 9 characterized by inspecting the justification of the right generation password of activation received from said order management machine.
[Claim 13] It connects with one or more software effectors which perform offered software, and each software effector through a communication

path. It is the software protection system equipped with the order management machine which manages the order of software received from each software effector. And each aforementioned software effector An effector ID storing means to store the effector ID of a proper, and the 1st confidential information storing means which stores the effector confidential information of a proper, The order creation means which creates the ordering information of the right of activation of one or more software, and carries out are recording maintenance is included. Said effector ID and said ordering information It is sent to said order management machine through said channel. Said order management machine The 1st module storing means which stores the 1st right generation module of activation, The 2nd confidential information storing means which stores all the effector confidential information stored in each aforementioned software effector, The 1st count means which calculates the value depending on the ordering information from said software effector, and the effector confidential information gained from said 2nd confidential information storing means, By changing said 1st right generation module of activation using the count result of said 1st count means A right generation password generation means of activation to generate the right generation password of activation is included. Said right generation password of activation It is sent to said software effector through said channel. Each software effector The 2nd module storing means which furthermore stores the 2nd right generation module of activation, The 2nd count means which calculates the value for which it depended on said order creation means at the ordering information by which are recording maintenance was carried out, and the effector confidential information stored in said 1st confidential information storing means, Using the count result of said 2nd count means by carrying out inverse transformation of the right generation password of activation from said order management machine A right generation password inverse transformation means of activation to generate the 1st right generation module of activation, The 1st right generation module of activation generated by said right generation password inverse transformation means of activation, A right generation means of activation to generate the right of activation of software based on the ordering information by which are recording maintenance was carried out at said order creation means using the 2nd right generation module of activation stored in said 2nd module storing means, The software protection system which includes a module elimination means to eliminate the first right generation module of activation, and a software activation means to perform software with which said right of activation

exists according to the execution condition shown in the right of activation concerned, after the right generation of activation.
[Claim 14] The 1st right generation module of activation stored in said 1st module storing means It has predetermined DS and semantics. Said right generation means of activation Only when the inverse transformation result of said right generation password inverse transformation means of activation has the 1st [said] same DS and semantics as the right generation module of activation, the 1st right generation module of activation, The software protection system according to claim 13 characterized by generating the right of activation of software based on the ordering information by which are recording maintenance was carried out at said order creation means using the 2nd right generation module of activation.
[Claim 15] Said order management machine includes further the 3rd confidential information storing means which stores the confidential information used for a public key signature method. Said right generation password generation means of activation By changing said 1st right generation module of activation using the count result of said 1st count means, and the confidential information stored in said 3rd confidential information storing means The right generation password of activation by which the digital signature was carried out with the public key signature method is generated. Said software effector A public information storing means to store the public information corresponding to the confidential information used for said public key signature method is included further. Said right generation password inverse transformation means of activation The software protection system according to claim 13 characterized by carrying out inverse transformation of the right generation password of activation from said order management machine using the count result of said 2nd count means, and said public information with the signature check method corresponding to said public key signature method.
[Claim 16] The software with which said software effector is provided It is enciphered including software proper information. Said right generation means of activation When said right generation password verification means of activation checks the justification of the right generation password of activation from said order management machine, By decoding the encryption software corresponding to the ordering information by which are recording maintenance was carried out for said order creation means, acquiring said software proper information, and enciphering this acquired software proper information by said effector confidential information The right of activation of the ordered software

is generated. Said software activation means Decode the encryption software corresponding to the ordering information by which are recording maintenance was carried out for said order creation means, and software and software proper information are acquired. The software protection system according to claim 1 to 15 characterized by performing decoded software only when the software proper information which decoded said right of activation using effector confidential information, acquired software proper information, and was acquired by these decode is in agreement.

[Claim 17] Said order creation means is a software protection system according to claim 1 to 15 which carries out are recording maintenance of the created ordering information in un-volatilizing, and is characterized by eliminating the ordering information concerned after generating the right of activation of the software with which said right generation means of activation corresponds.

[Claim 18] Said software effector and said order management machine are a software protection system according to claim 1 to 15 characterized by holding the hysteresis of the information exchanged mutually, respectively.

[Claim 19] It is the software protection system according to claim 1 to 15 which said software effector and said order management machine hold the code corresponding to the combination of all software as a table, and is characterized by said software effector sending the code obtained from said table to said order management machine as said ordering information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] About a software protection system, more specifically, this invention distributes software in the inactive condition, and relates to the software protection system which acquires the right of activation for activating software using channels, such as a telephone.

[0002]

[Description of the Prior Art] In recent years, various multimedia devices are developed and the onerous multimedia software of many

including a game or the software for education is sold. However, protection of the software is imperfect and the present condition is that many software copied unjustly has appeared on the market. Although there is regulation of laws, such as Patent Law and the Copyright Act, in order to prevent such an illegal copy, the protection of software from a mechanism side is strongly requested from coincidence.

[0003] For example, by the copy function currently offered by OS (operating system), there is an approach which can be made not to do a duplicate by making special a format of the record medium which stores software, such as a floppy disk. However, if the copy tool of the type which copies for every bit also by such approach is used, in many cases, it can reproduce. Moreover, for the user of normal, it also produces un-arranging [that backup cannot be made].

[0004] Moreover, the method of enciphering software and performing anti-copying is proposed. In this approach, it is enciphered and software is distributed among a user in the inactive condition. And the right of activation for activating the software by the specific device (the following conventional examples encryption file key) is distributed by order of a user. Since this right of activation is the information depending on a specific device, it cannot activate the same software by other devices using this. This approach is indicated by JP,2-60007,B. The configuration is shown in drawing 6 . In addition, this drawing 6 takes out a required part from Fig. 1st-6 of JP,2-60007,B on explanation, and resummarizes it in one drawing.

[0005] This software protection system is equipped with the software effector 601 which performs software, and the order management machine 602 which distributes software to the software effector 601 in drawing 6 .

[0006] The software effector 601 The encryption software storing section 603 and the order creation section 604, The effector ID storing section 605 and the code key storing section 606 which stores the effector code key of the proper corresponding to Effector ID, The encryption file key storing section 607 which stores the encryption file key received from the order management machine 602, The encryption file key decode section 608 which decodes an encryption file key by the effector code key, and gains a file key, and the software decode activation section 609 which decodes and performs encryption software using a file key are included. Such a software effector 601 of a configuration tells the order management machine 602 that Effector ID is an order in the order creation section 604, and the encryption file key for performing encryption software is required.

[0007] The order management machine 602 contains the file key storing section 610 which stores the file key of all software, the effector code key storing section 611 which stores the effector code key of all software effectors, and the encryption file key generation section 612 which enciphers by the effector code key of assignment of a file key, and generates an encryption file key. Such an order management machine 602 of a configuration takes out the file key of the software specified from the software effector 601 from the file key storing section 610, and takes out the code key corresponding to Effector ID from the effector code key storing section 611.

[0008] Next, actuation of the conventional software protection system shown in drawing 6 is explained. Encryption software enciphers the original software by the file key of a software proper. Two or more these encryption software is packed, is beforehand stored in record media, such as CD-ROM, for example, and is distributed among the software effector 601. The distributed encryption software is stored in the encryption software storing section 603. Encryption software is inactive software whose activation is impossible only now. In wishing to perform, it places an order by notifying ID which specifies ID of the software of an order and is stored in the effector ID storing section 605 in the order creation section 604 to the order management machine 602. In addition, this order is performed using a telephone etc. practical.

[0009] In the order management machine 602, the file key storing section 610 stores the file key of all software by making software ID into an index. Moreover, the effector code key storing section 611 has stored and managed all effector code keys by making Effector ID into an index. And the order management machine 602 which received the order from the software effector 601 gains the file key of the software of an order from the file key storing section 610, in the encryption FIIRUKI generation section 612, enciphers this file key by the code key of the effector of relevance, and creates an encryption file key. And this encryption file key is notified to the software effector 601.

[0010] The software effector 100 which received the encryption file key stores this in the encryption file key storing section 107. And at the time of software activation, the encryption file key decode section 108 decodes the encryption file key stored in the encryption file key storing section 107 by its code key in which it was stored by the effector code key storing section 106, and gains a file key. The software decode activation section 109 decodes encryption software by the file key called for in the encryption file key decode section 108,

and performs software. In addition, since an encryption file key is information effective only in the effector, use is impossible even if gained from a channel or the storing section by others.
[0011]
[Problem(s) to be Solved by the Invention] However, in the above conventional software protection systems, if order of software and reception of an encryption file key shall be altogether performed through a telephone, the information it is reported by telephone that explains below will increase, and it will become what lacked in practicality.
[0012] First, the number of bits of a file key and an effector code key is described. A file key is a key for enciphering the original software. Moreover, as for an effector code key, by the way, it is common to encryption here to use [which is a key for enciphering this file key] a private key block cipher. DES (Data Encryption Standard) which is the cipher system which has spread most in the U.S. as a private key block cipher, FEAL (Fast data Encipherment Algorithm) developed with the book later [the] are mentioned. Even when adopting which [these] cipher system, in order to secure safety, it is recognition in the present condition that about 64 bits of numbers of bits of a key are the need. Therefore, a file key and an effector code key serve as about 64-bit data, respectively. In addition, about DES, it is FIP. PUB 46 NBS About FEAL, it is A.Shimizu to Jan. and 1977. & S.Miyaguchi: "Fast Data Encipherment Algorithm FEAL" Advances in Cryptology-EUROCRYPT'87 It is stated to the detail at the Springer bookstore, respectively.
[0013] Next, the number of bits of an encryption file key is described. An encryption file key enciphers a file key by the effector code key. As mentioned above, since the file key and the effector code key are required for about 64 bits, this encryption file key also serves as a value of about 64 bits. 64 bits is about about 20 figures, supposing it expresses with the figure of a decimal. By the way, this encryption file key is orally told by the telephone to the user who operates the software effector 601 from the operator who operates the order management machine 602. Furthermore, the operator of the software effector 601 needs to input the told encryption file key into the software effector 601. However, if it becomes a digit long in this way, a mistake is made in saying, and it will be heard wrong, possibility of changing between inputs will become very large, and a problem will arise practical.
[0014] On the contrary, if the digit count of an encryption file key is made small in consideration of the above-mentioned practicality, in

connection with this, the number of bits of a file key or an activation code key will decrease, and safety will fall.
[0015] Moreover, in the above-mentioned conventional example, one encryption file key corresponds to the order of one software. Therefore, to the order of the software of N individual, the amount of information to tell becomes N times.
[0016] in addition, in the above-mentioned conventional example, once gaining the encryption file key to software, the software can be performed any number of times -- so to speak, it is "a right acquisition type of activation." However, the gestalt which pays a tariff according to the amount of the software used depending on the class of software may be more convenient rather. With this gestalt, activation of only a predetermined count is attained, for example using the right of activation received from the order management machine.
[0017] The 1st purpose of this invention is offering the software protection system which can reduce the amount of information between a software effector and an order management machine (for example, ** which does not reduce the number of bits of the key of a code), without degrading safety.
[0018] The 2nd purpose of this invention is offering the software protection system [like / (that is, the amount of information in the case of ordering the software of N individual becomes the same as the amount of information in the case of ordering one piece software)] for which the amount of information between a software effector and an order management machine does not depend on the number of the software to order.
[0019] The 3rd purpose of this invention is offering the software protection system which corresponds to conditional rights of activation, such as a count limit, flexibly.
[0020]
[Means for Solving the Problem] One or more software effectors which perform software with which invention concerning claim 1 was offered, It is the software protection system equipped with the order management machine which manages the order of software which connected with each software effector through the communication path, and was received from each software effector. An effector ID storing means by which each software effector stores the effector ID of a proper, The 1st confidential information storing means which stores the effector confidential information of a proper, and the order creation means which creates the ordering information of the right of activation of one or more software, and carries out are recording maintenance are included.

Effector ID and ordering information are sent to an order management machine through a channel. An order management machine The 2nd confidential information storing means which stores all the effector confidential information stored in each software effector, The effector confidential information corresponding to the effector ID received from the software effector is gained from the 2nd confidential information storing means. A right generation password generation means of activation to generate the right generation password of activation depending on the ordering information received from this effector confidential information and software effector that were gained is included. The right generation password of activation is sent to a software effector through a channel. Each software effector A right generation password verification means of activation to inspect the justification of the right generation password of activation furthermore received from the order management machine using the ordering information by which are recording maintenance was carried out, and the effector confidential information stored in the 1st confidential information storing means for the order creation means, When the justification of the right generation password of activation is checked as a result of inspection by the right generation password verification means of activation A right generation means of activation to generate the right of activation of the software an order with an order creation means for was placed based on the ordering information by which are recording maintenance was carried out, and a software activation means to perform software with which the right of activation exists according to the execution condition shown in the right of activation concerned are included.

[0021] Invention concerning claim 2 is set to invention of claim 1. The right generation password generation means of activation The ordering information received from the software effector, and the effector confidential information gained from the 2nd confidential information storing means It inputs into a data compression function with which an output is related to all the input bits, and the output of this data compression function is outputted as a right generation password of activation. The right generation password verification means of activation The ordering information by which are recording maintenance was carried out, and the effector confidential information stored for the 1st confidential information storing means for an order creation means It inputs into the same data compression function as the data compression function used with the right generation password generation means of activation, and when in agreement with the right generation

password of activation which the output received from the order management machine, it is characterized by judging that the right generation password of activation concerned is just.
[0022] Invention concerning claim 3 is set to invention of claim 1. An order management machine The 3rd confidential information storing means which stores the confidential information used for a public key signature method is included further. The right generation password generation means of activation The confidential information stored in the 3rd confidential information storing means, and the effector confidential information gained from the 2nd confidential information storing means, It uses with the ordering information received from the software effector, and the right generation password of activation by which the digital signature was carried out with the public key signature method is generated. A software effector A public information storing means to store the public information corresponding to the confidential information used for a public key signature method is included further. The right generation password verification means of activation With the signature check method corresponding to a public key signature method using the public information stored in the public information storing means, the ordering information by which are recording maintenance was carried out at the order creation means, and the effector confidential information stored for the 1st confidential information storing means It is characterized by inspecting the justification of the right generation password of activation received from the order management machine.
[0023] One or more software effectors which perform software with which invention concerning claim 4 was offered, It is the software protection system equipped with the order management machine which manages the order of software which connected with each software effector through the communication path, and was received from each software effector. An effector ID storing means by which each software effector stores the effector ID of a proper, The 1st confidential information storing means which stores the effector confidential information of a proper, and the order creation means which creates the ordering information of the right of activation of one or more software, and carries out are recording maintenance, The change value generation means which generates the change value which changes whenever ordering information is created with an order creation means, and carries out are recording maintenance is included. Effector ID, ordering information, and a change value It is sent to an order management machine through a channel. An order management machine The 2nd confidential information storing means which

stores all the effector confidential information stored in each software effector, The effector confidential information corresponding to the effector ID received from the software effector is gained from the 2nd confidential information storing means. A right generation password generation means of activation to generate the right generation password of activation depending on this gained effector confidential information, the ordering information received from the software effector, and a change value is included. The right generation password of activation is sent to a software effector through a channel. Each software effector The ordering information by which are recording maintenance was furthermore carried out at the order creation means, and the change value by which are recording maintenance was carried out at the change value generation means, A right generation password verification means of activation to inspect the justification of the right generation password of activation received from the order management machine using the effector confidential information stored in the 1st confidential information storing means, When the justification of the right generation password of activation is checked as a result of inspection by the right generation password verification means of activation A right generation means of activation to generate the right of activation of the software an order with an order creation means for was placed based on the ordering information by which are recording maintenance was carried out, and a software activation means to perform software with which the right of activation exists according to the execution condition shown in the right of activation concerned are included.
[0024] Invention concerning claim 5 is set to invention of claim 4. The right generation password generation means of activation The ordering information and the change value which were received from the software effector, and the effector confidential information gained from the 2nd confidential information storing means It inputs into a data compression function with which an output is related to all the input bits, and the output of this data compression function is outputted as a right generation password of activation. The right generation password verification means of activation The ordering information by which are recording maintenance was carried out at the order creation means, and the change value by which are recording maintenance was carried out at the change value generation means, The effector confidential information stored in the 1st confidential information storing means is inputted into the same data compression function as the data compression function used with the right generation password generation means of activation. When the output is in agreement with the right generation password of

activation received from the order management machine, it is characterized by judging that the right generation password of activation concerned is just.

[0025] One or more software effectors which perform software with which invention concerning claim 6 was offered, It is the software protection system equipped with the order management machine which manages the order of software which connected with each software effector through the communication path, and was received from each software effector. An effector ID storing means by which each software effector stores the effector ID of a proper, The 1st confidential information storing means which stores the effector confidential information of a proper, and the order creation means which creates the ordering information of the right of activation of one or more software, and carries out are recording maintenance, The 1st time stump generation means which generates a time stump and carries out are recording maintenance whenever ordering information is created with an order creation means is included. Effector ID and ordering information It is sent to an order management machine through a channel. An order management machine The 2nd time stump generation means which will generate a time stump if Effector ID and ordering information are received from a software effector, The 2nd confidential information storing means which stores all the effector confidential information stored in each software effector, The effector confidential information corresponding to the effector ID received from the software effector is gained from the 2nd confidential information storing means. This gained effector confidential information, A right generation password generation means of activation to generate the right generation password of activation depending on the ordering information received from the software effector and the time stump generated with the 2nd time stump generation means is included. The right generation password of activation is sent to a software effector through a channel. Each software effector The ordering information by which are recording maintenance was furthermore carried out at the order creation means, and the time stump by which are recording maintenance was carried out at the 1st time stump generation means, A right generation password verification means of activation to inspect the justification of the right generation password of activation received from the order management machine using the effector confidential information stored in the 1st confidential information storing means, When the justification of the right generation password of activation is checked as a result of inspection by the right generation password verification means of activation A right generation means of activation to generate the right

of activation of the software an order with an order creation means for was placed based on the ordering information by which are recording maintenance was carried out, and a software activation means to perform software with which the right of activation exists according to the execution condition shown in the right of activation concerned are included.

[0026] One or more software effectors which perform software with which invention concerning claim 7 was offered, It is the software protection system equipped with the order management machine which manages the order of software which connected with each software effector through the communication path, and was received from each software effector. An effector ID storing means by which each software effector stores the effector ID of a proper, The 1st confidential information storing means which stores the effector confidential information of a proper, and the order creation means which creates the ordering information of the right of activation of one or more software, and carries out are recording maintenance, The order authentication information generation means which generates the order authentication information depending on ordering information and effector confidential information, and carries out are recording maintenance is included. Effector ID, ordering information, and order authentication information It is sent to an order management machine through a channel. An order management machine The 2nd confidential information storing means which stores all the effector confidential information stored in each software effector, The effector confidential information corresponding to the effector ID received from the software effector is gained from the 2nd confidential information storing means. This gained effector confidential information, the ordering information received from the software effector, and order authentication information are used. An effector authentication means to perform authentication of a software effector and ordering information, and to treat the order authentication information concerned as order identification information which identifies an order when this authentication result is just, Only when the authentication result in an effector authentication means is just, a right generation password generation means of activation to generate the right generation password of activation depending on ordering information and order identification information is included. The right generation password of activation with order identification information It is sent to a software effector through a channel. Each software effector A right generation password verification means of activation to inspect the justification of the right generation password of activation received from the order

management machine using the ordering information by which are recording maintenance was carried out, and the order authentication information by which are recording maintenance was carried out at the order authentication information generation means for the order creation means furthermore, When the justification of the right generation password of activation is checked as a result of inspection by the right generation password verification means of activation A right generation means of activation to generate the right of activation of the software an order with an order creation means for was placed based on the ordering information by which are recording maintenance was carried out, and a software activation means to perform software with which the right of activation exists according to the execution condition shown in the right of activation concerned are included.

[0027] Invention concerning claim 8 is set to invention of claim 7. An order authentication information generation means The ordering information created by the order creation means, and the effector confidential information stored in the 1st confidential information storing means It inputs into a data compression function with which an output is related to all the input bits, and the output of this data compression function is outputted as order authentication information. An effector authentication means The effector confidential information gained from the 2nd confidential information storing means, and the ordering information received from the software effector It inputs into the same data compression function as the data compression function used with the order authentication information generation means. When the output of this data compression function is in agreement with the order authentication information received from the software effector It attests that the software effector and ordering information which placed an order are just. The right generation password generation means of activation The ordering information and the order identification information which were received from the software effector are inputted into the same data compression function as the data compression function used with the order authentication information generation means. The output of this data compression function is outputted as a right generation password of activation. The right generation password verification means of activation The ordering information by which are recording maintenance was carried out, and the order authentication information by which are recording maintenance was carried out at the order authentication information generation means for an order creation means It inputs into the same data compression function as the data compression function used with the order authentication information

generation means, and when in agreement with the right generation password of activation which the output received from the order management machine, it is characterized by judging that the right generation password of activation concerned is just.

[0028] One or more software effectors which perform software with which invention concerning claim 9 was offered, It is the software protection system equipped with the order management machine which manages the order of software which connected with each software effector through the communication path, and was received from each software effector. An effector ID storing means by which each software effector stores the effector ID of a proper, The 1st confidential information storing means which stores the effector confidential information of a proper, and the order creation means which creates the ordering information of the right of activation of one or more software, and carries out are recording maintenance, The change value generation means which generates the change value which changes whenever ordering information is created with an order creation means, and has predetermined DS or semantics, and carries out are recording maintenance, By calculating the value depending on ordering information and effector confidential information, and changing a change value with this calculated value The order authentication information generation means which generates order authentication information and carries out are recording maintenance is included. Effector ID, ordering information, and order authentication information It is sent to an order management machine through a channel. An order management machine The 2nd confidential information storing means which stores all the effector confidential information stored in each software effector, The effector confidential information corresponding to the effector ID received from the software effector is gained from the 2nd confidential information storing means. The inverse transformation means which calculates the value depending on this effector confidential information and ordering information from a software effector that were gained, and carries out inverse transformation of the order authentication information from a software effector using this value, An effector authentication means to attest that a software effector and ordering information are just when it has the DS or semantics as a change value of an inverse transformation means with the same output, Only when the authentication result in an effector authentication means is just, a right generation password generation means of activation to generate the right generation password of activation depending on ordering information is included. The right generation password of activation is sent to a software effector through

a channel. Each software effector A right generation password verification means of activation to inspect the justification of the right generation password of activation received from the order management machine using the ordering information by which are recording maintenance was carried out, and the order authentication information by which are recording maintenance was carried out at the order authentication information generation means for the order creation means furthermore, When the justification of the right generation password of activation is checked as a result of inspection by the right generation password verification means of activation A right generation means of activation to generate the right of activation of the software an order with an order creation means for was placed based on the ordering information by which are recording maintenance was carried out, and a software activation means to perform software with which the right of activation exists according to the execution condition shown in the right of activation concerned are included.

[0029] Invention concerning claim 10 is set to invention of claim 9. An order authentication information generation means The ordering information created by the order creation means, and the effector confidential information stored in the 1st confidential information storing means It inputs into a data compression function with which an output is related to each input bits of all, and the exclusive OR of the output and change value is outputted as order authentication information. An inverse transformation means The ordering information from a software effector, and the effector confidential information gained from the 2nd confidential information storing means By inputting into the same data compression function as the data compression function used with the order authentication information generation means, and calculating the exclusive OR of the output and order authentication information from a software effector Inverse transformation of the order authentication information concerned is carried out. The right generation password generation means of activation The ordering information and the order identification information which were received from the software effector are inputted into the same data compression function as the data compression function used with the order authentication information generation means. The output of this data compression function is outputted as a right generation password of activation. The right generation password verification means of activation The ordering information by which are recording maintenance was carried out, and the order authentication information by which are recording maintenance was carried out at the order authentication information generation means for

an order creation means It inputs into the same data compression function as the data compression function used with the order authentication information generation means, and when in agreement with the right generation password of activation which the output received from the order management machine, it is characterized by judging that the right generation password of activation concerned is just.

[0030] Invention concerning claim 11 is set to invention of claims 7 or 9. The right generation password generation means of activation In addition to the ordering information received from the software effector, the right generation password of activation depending on the effector confidential information gained from the 2nd confidential information storing means is generated. The right generation password verification means of activation is characterized by inspecting the justification of the right generation password of activation received from the order management machine using the ordering information by which are recording maintenance was carried out, and the effector confidential information stored in the 1st confidential information storing means for an order creation means.

[0031] Invention concerning claim 12 is set to invention of claims 7 or 9. An order management machine The 3rd confidential information storing means which stores the confidential information used for a public key signature method is included further. The right generation password generation means of activation The confidential information stored in the 3rd confidential information storing means, and the effector confidential information gained from the 2nd confidential information storing means, The right generation password of activation by which the digital signature was carried out with the public key signature method is generated using the ordering information and the order authentication information which were received from the software effector. A software effector A public information storing means to store the public information corresponding to the confidential information used for a public key signature method is included further. The right generation password verification means of activation The public information stored in the public information storing means, and the ordering information by which are recording maintenance was carried out at the order creation means, It carries out inspecting the justification of the right generation password of activation received from the order management machine with the signature check method corresponding to a public key signature method using the order authentication information by which are recording maintenance was carried out, and the effector confidential information stored for the 1st confidential information storing means

for an order authentication information generation means as the description.

[0032] One or more software effectors which perform software with which invention concerning claim 13 was offered, It is the software protection system equipped with the order management machine which manages the order of software which connected with each software effector through the communication path, and was received from each software effector. An effector ID storing means by which each software effector stores the effector ID of a proper, The 1st confidential information storing means which stores the effector confidential information of a proper, and the order creation means which creates the ordering information of the right of activation of one or more software, and carries out are recording maintenance are included. Effector ID and ordering information are sent to an order management machine through a channel. An order management machine The 1st module storing means which stores the 1st right generation module of activation, The 2nd confidential information storing means which stores all the effector confidential information stored in each software effector, By changing the 1st right generation module of activation using the count result of the 1st count means which calculates the value depending on the ordering information from a software effector, and the effector confidential information gained from the 2nd confidential information storing means, and the 1st count means A right generation password generation means of activation to generate the right generation password of activation is included. The right generation password of activation It is sent to a software effector through a channel. Each software effector The 2nd module storing means which furthermore stores the 2nd right generation module of activation, The 2nd count means which calculates the value for which it depended on the order creation means at the ordering information by which are recording maintenance was carried out, and the effector confidential information stored in the 1st confidential information storing means, Using the count result of the 2nd count means by carrying out inverse transformation of the right generation password of activation from an order management machine A right generation password inverse transformation means of activation to generate the 1st right generation module of activation, The 1st right generation module of activation generated by the right generation password inverse transformation means of activation, A right generation means of activation to generate the right of activation of software based on the ordering information by which are recording maintenance was carried out at the order creation means using the 2nd right generation module of activation stored in the

2nd module storing means, A module elimination means to eliminate the first right generation module of activation, and a software activation means to perform software with which the right of activation exists according to the execution condition shown in the right of activation concerned are included after the right generation of activation.

[0033] The 1st right generation module of activation with which invention concerning claim 14 is stored in the 1st module storing means in invention of claim 13 It has predetermined DS and semantics. The right generation means of activation Only when the inverse transformation result of the right generation password inverse transformation means of activation has the 1st same DS and semantics as the right generation module of activation, the 1st right generation module of activation, It is characterized by generating the right of activation of software based on the ordering information by which are recording maintenance was carried out at the order creation means using the 2nd right generation module of activation.

[0034] Invention concerning claim 15 is set to invention of claim 13. An order management machine The 3rd confidential information storing means which stores the confidential information used for a public key signature method is included further. The right generation password generation means of activation By changing the 1st right generation module of activation using the count result of the 1st count means, and the confidential information stored in the 3rd confidential information storing means The right generation password of activation by which the digital signature was carried out with the public key signature method is generated. A software effector A public information storing means to store the public information corresponding to the confidential information used for a public key signature method is included further. The right generation password inverse transformation means of activation It is characterized by carrying out inverse transformation of the right generation password of activation from an order management machine with the signature check method corresponding to a public key signature method using the count result of the 2nd count means, and public information.

[0035] The software with which a software effector is provided with invention concerning claim 16 in invention according to claim 1 to 15 It is enciphered including software proper information. The right generation means of activation When the right generation password verification means of activation checks the justification of the right generation password of activation from an order management machine, By decoding the encryption software corresponding to the ordering

information by which are recording maintenance was carried out for an order creation means, acquiring software proper information, and enciphering this acquired software proper information by effector confidential information The right of activation of the ordered software is generated. A software activation means Decode the encryption software corresponding to the ordering information by which are recording maintenance was carried out for an order creation means, and software and software proper information are acquired. Only when the software proper information which decoded the right of activation using effector confidential information, acquired software proper information, and was acquired by these decode is in agreement, it is characterized by performing decoded software.

[0036] In invention according to claim 1 to 15, an order creation means carries out are recording maintenance of the created ordering information in un-volatilizing, and after invention concerning claim 17 generates the right of activation of the software with which the right generation means of activation corresponds, it is characterized by eliminating the ordering information concerned.

[0037] It is characterized by invention concerning claim 18 holding the hysteresis of the information with which the software effector and the order management machine were exchanged mutually, respectively in invention according to claim 1 to 15.

[0038] Invention concerning claim 19 holds the code corresponding to the combination of all software in a software effector and an order management machine as a table in invention according to claim 1 to 15, and a software effector is characterized by sending the code obtained from the table to an order management machine as ordering information.

[0039]

[Function] In invention concerning claim 1, a software effector places an order for software by generating Effector ID and ordering information and sending these to an order management machine. An order management machine generates the right generation password of activation depending on the received ordering information and the effector confidential information corresponding to Activation ID which is information, and sends it to a software effector. This right generation password of activation judges whether they are the ordering information previously sent to the order management machine, their own effector confidential information, and the adjusted no, and when it has consistency, a software effector generates the right of activation of the software corresponding to ordering information, and performs the software concerned. Thus, since only the information which gives authorization

for the right generation password of activation, i.e., a software effector, to generate the right of software activation corresponding to ordering information is sent to a software effector from an order management machine, compared with the case where the right of activation itself is sent, a digit count is reducible. Moreover, even if a software effector places an order for two or more software at once, the amount of information becomes the same as the amount of information at the time of placing an order for one software.

[0040] In invention concerning claim 2, an order management machine inputs into a predetermined data compression function (for example, Hash Function) the ordering information received from the software effector, and the effector confidential information corresponding to Effector ID, and outputs the output of this data compression function as a right generation password of activation. On the other hand, a software effector inputs into the same data compression function as the above the ordering information by which are recording maintenance was carried out inside, and its own effector confidential information, and when in agreement with the right generation password of activation which the output received from the order management machine, it is judged that the right generation password of activation concerned is just. Thus, since the right generation password of activation is generated using a data compression function, the digit count can be reduced further.

[0041] In invention concerning claim 3, an order management machine holds the confidential information used for a public key signature method, it is used for it with this confidential information, the effector confidential information corresponding to Effector ID, and the ordering information received from the software effector, and it generates the right generation password of activation by which the digital signature was carried out with the public key signature method. On the other hand, a software effector holds the public information corresponding to the confidential information used for a public key signature method, and inspects the justification of the right generation password of activation received from the order management machine with the signature check method corresponding to a public key signature method using this public information, ordering information, and its own effector confidential information. Thus, since the right generation password of activation by which the digital signature was carried out to the software effector is sent, it becomes almost impossible to forge the right generation password of activation by the software effector side, and a software protection system with very high safety can be realized.

[0042] In invention concerning claim 4, the change value which changes

whenever it creates ordering information is sent to an order management machine from a software effector with ordering information. And an order management machine generates the right generation password of activation depending on effector confidential information, ordering information, and a change value, and sends it to an order management machine. A software effector inspects the justification of the right generation password of activation using ordering information, a change value, and effector confidential information. Therefore, the right generation password of activation from an order management machine becomes effective only with the software effector holding a corresponding change value. Therefore, even if it creates the same order as a different stage and enters the former right generation password of activation, since the change value generated at the time of a next order differs from the change value generated at the time of a former order, the entered password does not become effective.

[0043] In invention concerning claim 5, an order management machine inputs ordering information, a change value, and effector confidential information into data compression functions, such as a Hash Function, and outputs the output of this data compression function as a right generation password of activation. On the other hand, a software effector inputs into the same data compression function as the above the ordering information, the change value, and effector confidential information which are held inside, and when in agreement with the right generation password of activation which the output received from the order management machine, it is judged that the right generation password of activation concerned is just. Thus, since the right generation password of activation is generated using a data compression function, the digit count can be reduced further.

[0044] In invention concerning claim 6, the time stump is used instead of the change value in claim 4. Since this time stump is held common to a software effector and an order management machine, it becomes unnecessary to send a change value to an order management machine from a software effector like claim 4.

[0045] In invention concerning claim 7, an order management machine side can perform authentication of ordering information and a software effector in advance of issue of the right generation password of activation by introducing the order authentication information depending on ordering information and effector confidential information. And when an authentication result is O.K., an order management machine treats the above-mentioned order authentication information as order identification information which identifies an order, generates the right generation

password of activation depending on these ordering information and order identification information, and sends it to a software effector. A software effector inspects the justification of the right generation password of activation received from the order management machine using the ordering information and the order authentication information which are held inside, when this inspection result is O.K., generates the right of activation of software and performs corresponding software.

[0046] In invention concerning claim 8, the software effector inputted ordering information and effector confidential information into data compression functions, such as a Hash Function, and has obtained the output of this data compression function as order authentication information. Moreover, an order management machine attests that a software effector and ordering information are just, when in agreement with the order authentication information that inputted into the same data compression function as the above effector confidential information and the ordering information received from the software effector, and the output received it from the software effector. Furthermore, an order management machine inputs ordering information and order identification information into the same data compression function as the above, outputs the output of this data compression function as a right generation password of activation, and sends it to a software effector. On the other hand, a software effector judges ordering information and order authentication information that the right generation password of activation concerned is just, when it inputs into the same data compression function as the above and the output is in agreement with the right generation password of activation from an order management machine.

[0047] In invention concerning claim 9, a software effector generates order authentication information by changing the change value which changes for every creation of ordering information, and has predetermined DS or semantics with the value depending on ordering information and effector confidential information. This order authentication information is sent to an order management machine with Effector ID and ordering information. An order management machine attests that a software effector and ordering information are just, when the value for which it depended on the effector confidential information corresponding to Effector ID and ordering information from the software effector is calculated, inverse transformation of the order authentication information from a software effector is carried out using this value and this inverse transformation result has the same DS or the semantics as the above-mentioned change value. And only when this

authentication result is just, an order management machine generates the right generation password of activation depending on ordering information, and sends it to a software effector. A software effector generates the right of activation of the ordered software, when the justification of the right generation password of activation received from the order management machine is inspected using the ordering information and the order authentication information which are held inside and the justification of the right generation password of activation is checked. A count limit function and a user authentication function can be realized without increasing the amount of information exchanged between a software effector and an order management machine by such configuration.

[0048] In invention concerning claim 10, the software effector inputted ordering information and effector confidential information into data compression functions, such as a Hash Function, and has acquired the exclusive OR of the output and change value as order authentication information. The order management machine is carrying out inverse transformation of the order authentication information concerned by inputting the ordering information from a software effector, and the effector confidential information corresponding to Effector ID into the same data compression function as the above, and calculating the exclusive OR of the output and order authentication information from a software effector. Moreover, an order management machine inputs the ordering information and the order identification information from a software effector into the same data compression function as the above, and he is trying to output the output of this data compression function as a right generation password of activation. A software effector inputs into the same data compression function as the above, and when in agreement with the right generation password of activation which the output received from the order management machine, it judges the ordering information and the order authentication information which are held inside that the right generation password of activation concerned is just.

[0049] In invention concerning claim 11, an order management machine generates the right generation password of activation depending on the ordering information received from the software effector, and the effector confidential information corresponding to Effector ID. On the other hand, a software effector inspects the justification of the right generation password of activation received from the order management machine using the ordering information and effector confidential information which are held inside.

[0050] In invention concerning claim 12, an order management machine generates the right generation password of activation by which the digital signature was carried out with the public key signature method using the confidential information used for a public key signature method, the effector confidential information corresponding to Effector ID, and the ordering information and the order authentication information which were received from the software effector, and sends it to a software effector. A software effector inspects the justification of the right generation password of activation received from the order management machine with the signature check method corresponding to a public key signature method using the public information corresponding to the confidential information used for a public key signature method, and the ordering information, the order authentication information and effector confidential information which are held inside. Thus, since the right generation password of activation by which the digital signature was carried out to the software effector is sent, it becomes almost impossible to forge the right generation password of activation by the software effector side, and a software protection system with very high safety can be realized.

[0051] In invention concerning claim 13, generation of the right of activation cannot be performed only by the 2nd right generation module of activation stored in the software effector side. An order management machine changes the 1st right generation module of activation for activating this 2nd right generation module of activation into the form for which it depended on ordering information and effector confidential information from the software effector, and sends it as a right generation password of activation. In a software effector side, when it is right ordering information and an effector, the 2nd right generation module of activation currently held inside can be activated using this right generation password of activation. In this case, even if a software effector tends to generate the right of activation unjustly, since the 2nd right generation module of activation runs short of the information for it in amount of information, injustice is not made. Therefore, a much more safe software protection system is realizable.

[0052] In invention concerning claim 14, the 1st right generation module of activation stored in the order management machine has predetermined DS and semantics, only when the inverse-transformation result of the right generation password of activation has the 1st same DS and semantics as the right generation module of activation, the 1st right generation module of activation and the 2nd right generation module of activation are used for a software effector, and it generates the right

of activation of software.
[0053] In invention concerning claim 15, an order management machine generates the right generation password of activation by which the digital signature was carried out with the public key signature method by changing the 1st right generation module of activation using the count result of the 1st count means which is a value depending on the confidential information used for a public key signature method, and ordering information and effector confidential information. On the other hand, a software effector carries out inverse transformation of the right generation password of activation from an order management machine with the signature check method corresponding to a public key signature method using the count result of the 2nd count means which is a value depending on the public information corresponding to the confidential information used for a public key signature method, and ordering information and effector confidential information.
[0054] In invention concerning claim 16, the software with which a software effector is provided is enciphered including software proper information. And a software effector generates the right of activation of the ordered software by decoding the encryption software corresponding to the ordering information currently held inside, acquiring software proper information, and enciphering this acquired software proper information by effector confidential information, when the justification of the right generation password of activation from an order management machine is checked. Moreover, a software effector performs decoded software, only when the software proper information which decoded the encryption software corresponding to the ordering information currently held inside, acquired software and software proper information, decoded the right of activation using effector confidential information, acquired software proper information, and was acquired by these decode is in agreement.
[0055] In invention concerning claim 17, after a software effector carries out are recording maintenance of the created ordering information in un-volatilizing and generates the right of activation of corresponding software, it eliminates the ordering information concerned. Only an order can be sent continuously for the time being, and activation of software can be controlled by this based on the right generation password of activation returned behind.
[0056] In invention concerning claim 18, the software effector and the order management machine hold the hysteresis of the information exchanged mutually, respectively. By this, the trouble produced behind can be coped with flexibly.

[0057] The software effector and the order management machine hold the code corresponding to the combination of all software as a table, and he is trying for a software effector to send the code obtained from the table to an order management machine as ordering information in invention concerning claim 19. By this, the amount of data of ordering information can be reduced further.
[0058]
[Example]
(1) The 1st example drawing 1 is the block diagram showing the configuration of the software protection system concerning the 1st example of this invention. The software protection system of this example is equipped with the software effector 101 which performs software, and the order management machine 102 which distributes software to the software effector 101 in drawing 1 .
[0059] The software effector 101 The encryption software storing section 3 and the order creation section 4, The effector ID storing section 5 and the effector code key storing section 6 which stores the effector code key (an example of effector confidential information) corresponding to Effector ID, The right generation password verification section 7 of activation which inspects the justification of the right generation password of activation received from the order management machine 102, The right generation section 8 of activation which generates the right of activation using an effector code key based on ordering information, the right storing section 9 of activation which stores the generated right of activation, and the software decode activation section 10 which decodes and performs the above-mentioned encryption software when the right of activation corresponding to the time of software activation is effective are included. In the software effector 101 of such a configuration, the ordering information created in the order creation section 4 and Effector ID are transmitted to the order management machine 102, and the right generation password of activation for performing encryption software is required.
[0060] On the other hand, the order management machine 102 contains the effector code key storing section 11 which stores the effector code key of all software effectors, and the right generation password generation section 12 of activation which generates the right generation password of activation depending on the effector cryptographic key of ordering information and the software effector of relevance.
[0061] Next, actuation of the software protection system of the 1st example shown in drawing 1 is explained. In addition, in the following explanation, human being who is operating them shall perform the

communication link between the software effector 101 and the order management machine 102 through a telephone.

[0062] First, the generation method of encryption software is explained. The authentication child authA of a proper is set to Software SoftA. And the authentication child authA is combined with SoftA, this combined data is enciphered using the common confidential information S (not shown) within a system, and encryption software is generated. When it expresses by the formula, the encryption software ESoftA is ESoftA=E (S, authA||SoftA).

It becomes. In addition, in an upper type, || shows association for the code function with which E (S, *) used S as the key. Similarly, also about other software SoftB, the authentication child authB of a proper is made to correspond and encryption software is created. Hereafter, two or more encryption software created in the same procedure is stored in CD-ROM of one sheet, and is beforehand distributed among the software effector 101. This encryption software is stored in the encryption software storing section 3 in the example of drawing 1 .

[0063] The user of the software effector 101 specifies the software which wishes to perform out of the software stored in the encryption software storing section 3 by operating the software effector 101. For example, it is at the condition of Software A and Software C. Responding, the order creation section 4 generates corresponding ordering information. This ordering information is once accumulated into the order creation section 4. And the user of the software effector 101 notifies by telephone that the effector ID of a proper (stored in the effector ID storing section 5) is this ordering information to the operator of the order management machine 102 at the software effector 101. An order is completed by this.

[0064] If the ordering information notified from the software effector 101 is inputted, the right generation password generation section 12 of activation in the order management machine 102 will attest the software effector 101 which placed an order first (or user authentication), next will gain the code key of the software effector 101 of relevance from the effector code key storing section 11. Next, the right generation password generation section 12 of activation combines the ordering information received from the software effector 101, and the effector code key gained from the effector code key storing section 11, and inputs it into the Hash Function which was able to define this joint data beforehand. The output of this Hash Function is told to the user of the software effector 101 by telephone as a right generation password of activation.

[0065] Here, a Hash Function is data compression mold cipher processing, and the output is dependent on all the bits of an input, and has the property in which a different input pair from which an output becomes the same cannot be found easily. The concrete configuration approach is described in detail by 225 pages, for example from 224 pages of Ikeno, the "present age code theory" of the Oyama collaboration, and the Institute of Electronics and Communication Engineers issue. In addition, the Hash Function used by this example makes an input the function compressed into the value of about 10 figures of decimals.
[0066] The user of the software effector 101 enters into the right generation password verification section 7 of activation the right generation password of activation received by telephone. The same Hash Function as using with the order management vessel 102 is stored in this right generation password verification section 7 of activation. And the right generation password verification section 7 of activation inputs the data which combined the ordering information accumulated into the order creation section 4 at this Hash Function, and the effector code key stored in the effector code key storing section 6. Next, the right generation password verification section 7 of activation compares the output of this Hash Function with the right generation password of activation obtained from the order management machine 102. When the contents which the order management machine 102 was actually told that the ordering information accumulated into the order creation section 4 was are differed from or the effector code key stored in the software effector 101 differs from the effector code key gained within the order management machine 102 at this time, this comparison result serves as NG (inequality).
[0067] Only when the inspection result in the above-mentioned right generation password verification section 7 of activation is O.K. (coincidence), the right generation section 8 of activation is started, and generates the right of activation. The approach is as follows. First, the right generation section 8 of activation takes out corresponding encryption software from the encryption software storing section 3 with reference to the ordering information accumulated into the order creation section 4. For example, if it assumes that ESoftA was taken out as encryption software, the right generation section 8 of activation will decode this taken-out encryption software ESoftA using the common private key S (not shown) within a system, and will obtain the corresponding authentication child authA. Next, it enciphers using the effector code key in which this authentication child authA is stored by the effector code key storing section 6, and the right generation

section 8 of activation stores in the right storing section 9 of activation the authentication child who got by this encryption as a right of activation. Generally, in the case of the software effector X equipped with the specific effector code key Sx, the right of activation of Software A is set to E (Sx, authA). Since this right of activation is enciphered by the code key Sx of an effector X proper, even when the general memory to which the read-out protection from the outside is not given is used as the right storing section 9 of activation, the problem of leakage of secrets is not produced.

[0068] In case software A is performed, the software decode activation section 10 decodes the encryption software ESoftA using the common private key S within a system first, and obtains the authentication children authA and SoftA. Next, the software decode activation section 10 takes out the right E of activation corresponding to Software A (Sx, authA) from the right storing section 9 of activation. Next, the software decode activation section 10 compares the value which decoded and acquired the right E of activation (Sx, authA) by the effector code key Sx with the authentication child who had got previously. And the software decode activation section 10 performs software SoftA, when both are in agreement.

[0069] As explained above, the 1st example of this invention is generating the right of activation which the order management machine was performing in the system conventionally by the software effector side (in the conventional example, it is equivalent to generation of an encryption file key). That is, in this example, the order management machine 102 has only the function to give motive authorization, to the right generation section 8 of activation. since the right generation password of activation used as authorization information is the output of the Hash Function depending on ordering information and the code key of an effector here -- the value of about 10 figures of decimals -- realizable -- a telephone -- a mistake is made in telling, **** between inputs decreases, and a user interface also becomes good. Moreover, authentication of ordering information and an effector is attained. Moreover, since the order management machine 102 only gives motive authorization to the right generation section 8 of activation, it is not dependent on the number of the software to order, and it can always realize the right generation password of activation by the small digit count.

[0070] Next, the safety to a malfeasance is explained in the software protection system of the 1st example of the above. In the system of the 1st example, in case the order management machine 102 publishes the

right generation password of activation to it in response to an order from the software effector 101, accounting corresponding to an order shall be made. Generally as the approach of payment, the approach of a credit etc. will be adopted. Therefore, in the software effector 101, if it is difficult to generate freely the inaccurate right of activation which is not set as the object of accounting, it will be said that the safety of a system is high.

[0071] First, it is possible as an attack from the outside for making the inaccurate right of activation generate to operate the right generation section 8 of activation in the software effector 101 independently. Moreover, the attack of making the right of activation of software other than the order created in the order creation section 4 create in the right generation section 8 of activation is also considered. To these attacks, when a user prevents from changing each component in the software effector 101, it can be coped with.

[0072] In the 1st example, an order is performed in the order creation section 4, and the right generation section 8 of activation will not be started, if it is not after passing through a series of activities that next inspection of the right generation password of activation corresponding to it passes. That is, in the 1st example, it cannot change so that only the right generation section 8 of activation may operate independently. Moreover, in the 1st example, it cannot operate only inspection of the right generation password of activation, and the right generation section 8 of activation except for order creation from a series of above-mentioned activities, either. Furthermore, in case the ordering information created in the order creation section 4 is used in the right generation password verification section 7 of activation, and the right generation section 8 of activation, in the any, a user cannot change the contents of ordering information. Therefore, in the 1st example, even if the above unjust attacks are delivered, the right of activation is not generated.

[0073] In addition, if it takes into consideration that the case where the software effector 101 is an appliance chiefly, and the case where the program in a software effector is realized by CD-ROM etc. are very common, it is based actually that a user prevents from changing each component in a software effector.

[0074] Moreover, in order to perform software unjustly, attack of entering the right generation password of activation received to a certain order as a right generation password of activation to another order, and inputting into software effectors other than the software effector which placed an order is also considered. However, since the

right generation password of activation is a value depending on ordering information and an effector code key, when a software effector differs from ordering information, inspection of the right generation password of activation does not pass along it by the system of the 1st example. Therefore, the 1st example can cope with it also to such an unjust attack.

[0075] Furthermore, in order to perform software unjustly, attack of entering the password of a value suitable in round robin is also considered to the right generation password of activation of a certain order. However, in the 1st example, since the digit count of a password is set as about 10 figures by the decimal, even if an inaccurate user enters a password suitably, it is thought that the probability for it to pass the Banking Inspection Department 7 by chance is close to 0 in practice. Therefore, the 1st example can cope with it also to such an attack.

[0076] Furthermore, in order to perform software unjustly, it is also considered that a user forges the right generation password of activation. To this, it can be coped with, for example using the public key signing method. Since the private key of the order management machine 102 is needed in order to generate the right generation password of activation when the public key signing method is used, a general user cannot do forgery of a password. Moreover, it can be coped with also by the approach of not exhibiting procedure (operation) for publishing the right generation password of activation. In the 1st example of the above, although the right generation password verification section 7 of activation in the software effector 2 inspects in the same procedure as generation of the right generation password of activation, the algorithm of the right generation password verification section 7 of activation is not opened to a user. Furthermore, since the right generation password verification section 7 of activation can use it independently (that is, the component in the software effector 101 is changed), the problem of password forgery is not produced.

[0077] Moreover, when the right storing section 9 of activation is constituted using general memory without a read-out protection function, generating the right of activation unjustly is also considered by analyzing the right of activation stored in the right storing section 9 of activation. However, in the 1st example, since it is enciphered by the code key of the corresponding software effector 101 and the effector code key is moreover set as about 64 bits, the right of activation stored in the right storing section 9 of activation cannot analyze the right of activation easily. Furthermore, safety can be raised more by

making it not exhibit decode processing to a user, or a user prevents from observing an effector code key.

[0078] The above explanation shows that it is impossible to forge the right of activation by the software effector 101 side as a matter of fact.

[0079] In addition, as the system which can carry out count use of infinity of the right of activation, i.e., a system of "the right acquisition type of activation", the system of the 1st example of the above is constituted, if a user gets the right of activation. Therefore, the multiple-times input of the right generation password of activation to the same ordering information may be carried out.

[0080] (2) The 2nd example drawing 2 is the block diagram showing the configuration of the software protection system concerning the 2nd example of this invention. Unlike the system of "a right acquisition type of activation" like the 1st example, this 2nd example becomes effective when conditions, such as for example, a count of activation, are added to the right of activation of software.

[0081] By the way, in order to restrict the count of activation of the ordered software, the right generation password of activation must become effective only at the time of the first input. This is because following un-arranging will arise if effective also at the time of the input of the 2nd henceforth. For example, a certain software effector creates the order which carries out N time activation of the software A, and presupposes that the right generation password of activation to the order concerned was got from the order management machine. If this password is entered into a software effector, the right of activation which can carry out N time activation of the software A will be generated. Next, when this right of activation decreases, the order which carries out N time activation of the software A again in the same software effector is created, and a former password is entered into an order management machine, without placing an order. If this password becomes effective and the right of activation of N time of Software A is generated again, the semantics of a limit of the count of activation will be lost substantially.

[0082] So, in the 2nd example, in order to confirm the right generation password of activation only at the time of the first input, in addition to the configuration of the 1st example, the value which changes for every order is introduced. That is, in the 2nd example, the change value from which a value changes each time is generated to each ordering information, and it is made effective [the right generation password of activation corresponding to this change value]. Although many things

are considered as the implementation approach of a change value of changing for this the order of every, he generates a random number for every order, and is trying to use this random number in the 2nd example as a change value which changes the whole order.

[0083] The software protection system of this example is equipped with the software effector 201 which performs software, and the order management machine 202 which distributes software to the software effector 201 in drawing 2 . The software effector 201 contains the encryption software storing section 3 and the order creation section 4 of the same configuration as the example of drawing 1 , the effector ID storing section 5, the effector code key storing section 6, the right generation section 8 of activation, the right storing section 9 of activation, and the software decode activation section 10. Furthermore, the software effector 201 contains the random-number generation machine 20 started at every order, and the right generation password verification section 21 of activation which confirms the justification of the received right generation password of activation using ordering information, an effector code key, and random-number data.

[0084] On the other hand, the order management machine 202 contains the effector code key storing section 11 of the same configuration as the example of drawing 1 . Furthermore, the order management machine 202 contains the right password generation section 22 of activation which generates the right generation password of activation depending on all them using the ordering information and the random number which were sent from the software effector 201, and the code key of the software effector 202 gained from the effector code key storing section 11.

[0085] As stated above, in this 2nd example, a random number new at every order is generated. And in addition to the 1st ordering information and Effector ID in an example, the user of the software effector 201 notifies the operator of the order management machine 202 of this random number by telephone. In addition, in order to make a user interface good, let this random number be the value of about 10 figures of decimals.

[0086] The right generation password generation section 22 of activation in the order management machine 202 inputs the data which combined the effector code key of ordering information, a random number, and the corresponding software effector 201 with the Hash Function same with having used in the 1st example. And the user of the software effector 201 is notified of the value of 10 figures of decimals which are the output of this Hash Function by telephone as a right generation password of activation.

[0087] The user of the software effector 201 which received the notice enters the above-mentioned right generation password of activation into the right generation password verification section 21 of activation of the software effector 201. The right generation password verification section 21 of activation combines the ordering information and the random number which were obtained from the order creation section 4 and the random-number-generation section 20, and the effector code key obtained from the order management machine 202, and inputs it into the Hash Function currently used with the order management vessel 202, and the same Hash Function. And the right generation password verification section 21 of activation starts the right generation section 8 of activation, only when both are in agreement as compared with the right generation password of activation into which the output of this Hash Function was inputted. Since the actuation after this is the same as that of the 1st example mentioned above, the explanation is omitted.
[0088] In the 2nd example of the above, a random number new at every order is generated automatically. And in the case of the procedure of normal, from the order management machine 202, the right generation password of activation depending on this random number (value which changes for every = order) is published. And this right creation password of activation becomes effective only in the software effector 201 holding a corresponding random number. Therefore, since the random number at the time of order generating of the 2nd henceforth differs from the random number generated at the time of the 1st order generating, the multiple-times unauthorized use of the right generation password of activation obtained at the time of the 1st order generating cannot be carried out. In addition, it is desirable that a user can change the above-mentioned random number freely, or prevents from setting it up in the 2nd example in addition to the management to the safety reservation explained in the 1st example.
[0089] In addition, when making it possible to once save an order, you may make it clear or update the random number which participates in it in the phase which generated the right of activation, although it consists of the 2nd example of the above as the former random number remains until a new order is created. By this, safety increases further.
[0090] (3) The 3rd example drawing 3 is the block diagram showing the configuration of the software protection system concerning the 3rd example of this invention. This 3rd example adds efficient effector authentication to the 1st above-mentioned example. The software protection system of the 3rd example is equipped with the software effector 301 which performs software, and the order management machine

302 which distributes software to the software effector 301 in drawing 3 .

[0091] The software effector 301 contains the encryption software storing section 3 and the order creation section 4 of the same configuration as the 1st above-mentioned example, the effector ID storing section 5, the effector code key storing section 6, the right generation section 8 of activation, the right storing section 9 of activation, and the software decode activation section 10. Furthermore, the software effector 301 contains the order authentication information generation section 30 which generates ordering information and the order authentication information depending on an effector code key, and the right generation password verification section 31 of activation which inspects the justification of the right generation password of activation received from the order management machine 302 using ordering information, an effector code key, and order authentication information.

[0092] On the other hand, the order management machine 302 contains the effector code key storing section 11 of the same configuration as the example of drawing 1 . Furthermore, ordering information and order authentication information that the order management machine 302 was received from the software effector 301, The effector authentication section 32 which attests a software effector using the effector code key gained from the effector code key storing section 11, When an effector authentication result is O.K., order authentication information is used as order identification information which identifies ordering information, and the right generation password generation section 33 of activation which generates the right generation password of activation using ordering information and order identification information (= order authentication information) further is included.

[0093] Next, actuation of the software protection system of the 3rd example shown in drawing 3 is explained. First, if ordering information is created in the order creation section 4 of the software effector 301, the order authentication information generation section 30 will input the data which combined ordering information and the effector code key obtained from the effector code key storing section 6 with the Hash Function same with having used in the 1st example. And in addition to ordering information and Effector ID, the user of the software effector 301 tells by telephone the operator of the order management machine 302 by making the output of the above-mentioned Hash Function into order authentication information. In addition, ordering information and order authentication information are accumulated in the order creation section 4 and the order authentication information generation section 30,

respectively.
[0094] First, the effector authentication section 32 uses as a key the effector ID received from the software effector 301, the effector code key storing section 11 is searched with the order management machine 302, and the effector code key of the corresponding software effector 301 is gained. Next, the effector authentication section 32 inputs the data which combined the ordering information received from the software effector 301, and an effector code key into the Hash Function same with using with the software effector 301. Next, the effector authentication section 32 compares the output of this Hash Function with the order authentication information received from the software effector 301. And only when the comparison result is in agreement, the effector authentication section 32 judges it as that to which a partner is a right effector and performed the right order, and uses order authentication information for management and transfer of ordering information and the information relevant to this as order identification information which identifies an order. Moreover, the right generation password generation section 33 of activation inputs into the same Hash Function as the above the data which combined ordering information and order identification information (= order authentication information). And as a right generation password of activation, the operator of the order management machine 302 makes the output of the Hash Function order identification information and a pair, and tells it by telephone to the user of the software effector 301.
[0095] The user of the software effector 301 enters the transmitted right generation password of activation into the right generation password verification section 31 of activation. It inspects whether it is in agreement with the right generation password of activation into which it responded, the right generation password verification section 31 of activation inputted into the Hash Function the data which combined the ordering information accumulated in the order creation section 4, and the order authentication information accumulated in the order authentication information generation section 30, and the output was inputted. And the right generation password verification section 31 of activation starts the right generation section 8 of activation, only when this inspection result is in agreement. The actuation after this is the same as that of the 1st example, and omits the explanation.
[0096] In the 3rd example of the above, the order management machine 302 performs authentication of ordering information and a software effector before issue of the right generation password of activation. Since accounting is made by order, the authentication function is required of

an actual system anyway. Although this authentication function can be separated from an order and it can also prepare separately, by the approach of challenging and attesting by the response to it, for example, the exchange of these challenges and a response will give a remarkable burden to the user of a software effector in practice. So, in the 3rd example, it is made to perform authentication of ordering information and a software effector to an order and coincidence efficiently. Therefore, in the 3rd example, the order authentication information depending on ordering information and the code key of an effector is introduced. And this order authentication information is added to ordering information and Effector ID, and is told to the order management machine 302. In addition, in the 3rd example of the above, since it is the output of a Hash Function, this order authentication information is realizable by about 10 figures of decimals, and also when telling by telephone, it does not give a user a burden so much.

[0097] The order management machine 302 is performing authentication of ordering information and the software effector 301 by using the above-mentioned order authentication information. That is, when the ordering information which the software effector 301 created in the order creation section 4 differs from the ordering information told to the order management machine 302 by telephone, NG is outputted in the effector authentication section 32 of the order management machine 302. Moreover, also when a certain software effector tells different information from its own effector ID by telephone, it can check in this effector authentication section 32.

[0098] Only when the above-mentioned authentication result is O.K., order authentication information is used for the order management machine 302 as order identification information for identifying an order. And the order management machine 302 generates the right generation password of activation corresponding to this order. This right generation password of activation is transmitted to the software effector 301. Since this right generation password of activation is also the output of a Hash Function, it is realizable by about 10 figures of decimals. In the software effector 301, the entered right generation password of activation is inspected using the ordering information and the order authentication information (= order identification information) which are stored in the interior. After passing through this inspection, the right of activation which becomes effective only with the specific software effector holding the order authentication information and ordering information corresponding to the entered right generation password of activation is generated. In addition, since the

information on an effector code key is already included in the order identification information (= order authentication information) of the right generation password of activation, the effector code key is not contained in the right generation password of activation itself here.
[0099] In addition to the information which should be transmitted in the 1st example at the time of an order, in the 3rd example of the above, the user of the software effector 301 has told order authentication information to the order management machine 302. By this, the order management machine 302 can perform authentication of ordering information and a software effector, before publishing the right generation password of activation. This order authentication information is the value of about 10 figures of decimals, and does not give a burden so much to the user of the software effector 301. Moreover, compared with the case where can realize authentication by the exchange of the same count as the 1st example, and user authentication is prepared separately, it is efficient. And this order authentication information is used for managing ordering information and the information related to it as order identification information which identifies ordering information.
[0100] (4) The 4th example drawing 4 is the block diagram showing the configuration of the software protection system concerning the 4th example of this invention. This 4th example adds an efficient effector authentication function to the 2nd example which introduced the random number. Like [the 4th example] the 2nd example, when conditions, such as a count of activation, are added to the right of activation of software, it becomes effective. The software protection system of the 4th example is equipped with the software effector 401 which performs software, and the order management machine 402 which distributes software to the software effector 401 in drawing 4 .
[0101] The software effector 401 contains the encryption software storing section 3 and the order creation section 4 of the same configuration as the 1st above-mentioned example, the effector ID storing section 5, the effector code key storing section 6, the right generation section 8 of activation, the right storing section 9 of activation, and the software decode activation section 10. Furthermore, the software effector 401 contains the random-number generation section 41 which generates a random number with the structure beforehand determined as the order hash section 40 which combines ordering information and an effector code key, and performs a hash operation, or semantics for every order, and the exclusive-OR section 42 which calculates the exclusive OR of the output of the random number concerned

and the order hash section 40.
[0102] On the other hand, the order management machine 402 contains the effector code key storing section 11 of the same configuration as the example of drawing 1 . Furthermore, the order hash section 44 which the order management machine 402 combines the ordering information received from the effector code key and the software effector 401 which were gained from the effector code key storing section 11, and performs the same hash operation as the software effector 401, The exclusive-OR section 45 which calculates the exclusive OR of the output of the order number received from the software effector 401, and the order hash section 44, The effector authentication section 46 which inputs the output of the exclusive-OR section 45 and attests the justification of the software effector 401, and the right generation password generation section 47 of activation which starts only when the authentication result of the effector authentication section 46 is O.K., and generates the right generation password of activation are included.
[0103] Next, actuation of the software protection system of the 4th example shown in drawing 4 is explained. First, in the software effector 401, if the order creation section 4 creates ordering information, the order hash section 40 will input the data which combined the ordering information concerned and the code key of the software effector obtained from the effector code key storing section 6 with the Hash Function same with having used in the 1st example. Moreover, the random-number generation section 41 generates random-number data with the structure defined beforehand or semantics. As an example, by this example, a triplet is set to "0" from the most significant of random-number data, and the triplet is set to "1" from the least significant. Other bits store a random number. It fixes beforehand between the others and order management machines 402 and the software effectors 401, and some data of Effector ID may be made to correspond to a part with that random-number data. [example / this] Next, the exclusive-OR section 42 calculates the exclusive OR of the output of the order hash section 40, and the random-number data generated in the random-number generation section 41. The user of the software effector 401 tells the operator of the order management machine 402 with ordering information and Effector ID by making the result of an operation of this exclusive-OR section 42 into order authentication information. In addition, if the number of bits of the above-mentioned random-number data is taken to the same extent as the output of the order hash section 40, order authentication information will serve as about 10 figures of decimals, and will give neither the user of the software effector 401, nor the operator of the

order management machine 402 so big a burden.
[0104] With the order management vessel 402, the effector authentication section 46 gains the code key of the software effector which corresponds from the effector code key storing section 11, combines this and ordering information, and inputs into the order hash section 44. And the exclusive-OR section 45 calculates an exclusive OR with the order authentication information thought to be the output of the order hash section 44 from the software effector 401. If ordering information and Effector ID are right, the output of the order hash section 44 will become the same as the output of the order hash section 40 in the software effector 401 which placed an order. Moreover, the output of the exclusive-OR section 45 becomes the same as the random-number data generated in the random-number generation section 41 of the software effector 401 which placed an order. That is, in now, the least significant to "0" and a triplet are set to "1" from the most significant of random-number data by the triplet. The effector authentication section 46 checks whether the output of the exclusive-OR section 45 has the structure and semantics of the random number defined beforehand, and if it is O.K., ordering information and an effector will attest it with the right. And only when this authentication result is O.K., the right generation password generation section 47 of activation generates the right generation password of activation. The actuation after this is the same as the 3rd example. That is, the right generation password of activation generated with the order management vessel 402 is transmitted to the software effector 401 by the telephone etc., it is inspected by the software effector side, and the right of activation of the software corresponding to the case of O.K. is created.
[0105] In the 4th example of the above, like the 2nd example, a random number is introduced and it can respond to the right generation of activation with a count limit. Furthermore, the 4th example is equipped with the user authentication function like the 3rd example. Thus, although the 4th example has the function of the 2nd and 3rd examples, the digit count of an especially random order number and the amount-of-data [which is exchanged between the software effector 401 and the order management machine 402] and right generation password of activation is not increasing it.
[0106] (5) The 5th example drawing 5 is the block diagram showing the configuration of the software protection system concerning the 5th example of this invention. In this 5th example, it has the right generation module of activation of an inactive condition in each software effector, that right generation module of activation is

activated with the right generation password of activation given from an order management machine, and it is characterized by generating the predetermined right of activation by that module. In addition, in the following explanation, the right generation module of activation is divided into two parts, the right generation module A of activation which is one of these is stored in a software effector, it is enciphered and a software effector receives another right generation module B of activation from an order management machine. As for these right generation modules A and B of activation, both can generate the predetermined right of activation for the first time together. Therefore, by the right generation module A of activation stored in the software effector, it is in an inactive condition and the right of activation cannot be generated.

[0107] The software protection system of the 5th example is equipped with the software effector 501 which performs software, and the order management machine 502 which distributes software to the software effector 501 in drawing 5 .

[0108] The software effector 501 contains the encryption software storing section 3 and the order creation section 4 of the same configuration as the 1st above-mentioned example, the effector ID storing section 5, the effector code key storing section 6, the right generation section 8 of activation, the right storing section 9 of activation, and the software decode activation section 10. Furthermore, the software effector 501 contains the order hash section 50 which combines ordering information and an effector code key, and performs a hash operation, the storing section 51 which stores the right generation module A of activation, the inverse transformation section 52 which carries out inverse transformation of the right generation password of activation received from the order management machine 502, and the storing section 53 which stores the inverse transformation result of the inverse transformation section 52. In addition, if ordering information and Effector ID are right, the right generation module B of activation will be stored in this storing section 53.

[0109] On the other hand, the order management machine 502 contains the effector code key storing section 11 of the same configuration as the example of drawing 1 . Furthermore, an order management machine 502 contains the order hash section 54 which combines the ordering information received from the software effector 501, and the code key of the effector of the relevance obtained from the effector code key storing section 11, and performs a hash operation, the storing section 55 which store in the right generation module B of activation, and the

right generation password generation section 56 of activation change a module B using the output of the order hash section 54, and generate the right generation password of activation.

[0110] Next, actuation of the software protection system of the 5th example shown in drawing 5 is explained. First, the user of the software effector 501 specifies the order of the software which wishes to perform by operating the software effector 501. Responding, the order creation section 4 creates corresponding ordering information. And the user concerned notifies the effector ID of a proper to ordering information and the software effector 501 by telephone etc. at the order management machine 502.

[0111] If the notice from the software effector 501 is received, based on Effector ID, the effector code key storing section 11 will be searched with the order management machine 502, and the code key of the corresponding software effector will be gained. Next, the order hash section 54 combines the ordering information received from the software effector 501, and the effector code key obtained from the effector code key storing section 11, and inputs it into the Hash Function same with having used in the 1st example. The right generation password generation section 56 of activation changes the right generation module B of activation by using as a key the hash value outputted from the order hash section 54, and publishes the right generation password of activation. The operator of the order management machine 502 transmits this right generation password of activation to the user of the software effector 501 by telephone etc.

[0112] Next, the user of the software effector 501 who received the right generation password of activation by telephone enters this password into the inverse transformation section 52 of the software effector 501. The order hash section 50 is equipped with the same Hash Function as having used with the order management vessel 502. And the order hash section 50 combines the ordering information accumulated into the order creation section 4, and the effector code key obtained from the effector code key storing section 6, and performs a hash operation to this joint data. The inverse transformation section 52 carries out inverse transformation of the right generation password of activation received from the order management machine 502 by using as a key the hash value outputted from the order hash section 50. If ordering information and an effector code key are just, the hash value outputted from the order hash section 50 will become the same as the hash value (output of the order hash section 54) in the order management machine 502. Therefore, the output of the inverse transformation section 52

serves as the right generation module B of activation. Next, the right generation section 8 of activation generates the right of activation corresponding to ordering information using the right generation module A of activation beforehand stored in the storing section 51, and the gained module B. After the right of activation is generated by the right generation section 8 of activation, Module B is deleted according to the right generation module of activation.

[0113] In the 5th example of the above, the right generation module A of activation beforehand stored in the software effector side is in an inactive condition, and cannot operate only now in amount of information. In the order management machine 502, the module B for activating this is changed into the form depending on the ordering information and the code key of a software effector, and is sent as a right generation password of activation. In the 1st - the 4th example which were mentioned above, the right generation module of activation existed in the software effector in the perfect form. However, in order to start this, authorization called the right generation password of activation was required. On the other hand, in the configuration of the 5th example, the right generation module of activation exists in a software effector in the condition of having run short in amount of information. For this reason, the 5th example has the more high safety to unjust generation of the right of activation compared with the 1st - the 4th example. In addition, Module B is deleted in order to return to the original condition, after the right generation modules A and B of activation generate the right of activation of an order.

[0114] In the 5th example, since the right generation module B of activation is changed depending on ordering information and the secret key of an effector, when orders differ or effectors differ, the user of a software effector cannot get the module B of normal. However, in the 5th example, since Module B is contained as information in the right generation password of activation, compared with the 1st in which only authorization information was included - the 4th example, it is necessary to increase the digit count of the right generation password of activation somewhat. In addition, the amount of data of the right generation password of activation in this 5th example is not dependent on the number of the software to order.

[0115] In addition, in the 5th example, this is immediately used for the software effector 501 as a module B after inverse transformation, without checking the right generation password of activation received from the order management machine 502. Therefore, when neither ordering information nor an effector code key suits the entered right generation

password of activation, the right generation module of activation does not operate correctly. Before supposing that it has specific structure and semantics with for example, the module B and using this after inverse transformation in the software effector 501 in a place, checking structure and semantics is also considered. For example, when it is instruction code with Module B, there must be specific structure in the code. Therefore, an error can be processed before activation of the right generation module of activation by confirming whether Module B has this specific structure.

[0116] In addition, the random number used in the example of the 2nd and 4 described above may be generated using a counter etc. that what is necessary is just the value which changes for every order. Moreover, it may replace with a random number and a time stump may be used. Since a time stump is possible (generating by the clock circuit is possible) in generating in common, it becomes unnecessary to send a change value from a software effector to an order management machine with a software effector and an order management vessel.

[0117] Moreover, in case the right generation password of activation is generated, you may make it make it dependent also on an effector code key in addition to ordering information and order identification information in the example of the 3rd and 4. Since only the order management machine knows its effector code key for a software effector in addition to itself, only an order management machine can make this right generation password of activation. Therefore, when the right generation password of activation can be considered as signature information on an order management machine and a trouble etc. arises, this information can be submitted to the 3rd person as a proof. Moreover, it may replace with the signature approach using such a secret key cryptosystem, and the signature approach using public key encryption may be used. In this case, an order management machine holds secret information and uses this secret information in the case of generation of the right generation password of activation. On the other hand, in a software effector side, the public information corresponding to the confidential information of an order management machine is held, and the justification of the right generation password of activation is checked using this. Since the justification of the right generation password of activation can be checked only when the confidential information of an order management machine is used, this right generation password of activation can be considered as a signature of an order management machine.

[0118] Moreover, in the 1-4th examples, although it is made to encipher

software by combining the original software SoftA and the corresponding authentication child authA, and enciphering this combined data with the key S common to a system, and although he was trying to use the data which enciphered this authentication child by the effector code key Sx as a right of activation, this invention is not limited to such an approach. For example, an authentication child and Effector ID may be combined and what enciphered this combined data with the key common to a system may be used as a right of activation. When a formula describes the right of activation of Effector X, it is E (S, authA || IDx).
It becomes. In this case, when the right of activation decodes the right of activation, and encryption software with a key common to a system, and the authentication child's obtained from both corresponds, and Effector ID is gained from the decode result of the right of activation and this is in agreement with the effector ID in an effector, it is attested, and it performs software. Anyway, this invention is applicable if it is the cipher system with which an effector can generate the right of activation using the data already held from encryption software.

[0119] Moreover, in the 1-4th examples of the above, although an order is placed by one message of a telephone and the right generation password of activation to it is received, this may be another message. That is, an order is first placed from a software effector to an order management machine, and this order is once saved. Next, an order management machine telephones a software effector, collates by the order number, and notifies the right generation password of activation. By this, the telephoned time amount becomes short for the user of a software effector, and it is convenient also in tariff. Moreover, the user of a software effector can work another software activation etc. until the right generation password of activation is notified from the user of an order management machine. On the other hand, user authentication can be performed by performing a call-back also for an order management machine.

[0120] Moreover, in the 1-4th examples of the above, when a software effector inspects the right generation password of activation and generates the right of activation, the ordering information saved beforehand is loaded and used. However, in order to reload ordering information and to make it not use a password again, after generating the right of activation first, it is necessary to eliminate the saved ordering information.

[0121] Moreover, in each above-mentioned example, it is possible by leaving the hysteresis of the exchange with a software effector and an order management machine on both sides to make it the reference works at

the time of the trouble about an order. Moreover, the user interface of order guidance can be made good by leaving what kind of software was purchased until now to the software effector side.

[0122] Moreover, in each above-mentioned example, although it was deciding to use ID of software for the condition of Software A and Software B as ordering information from a software effector to an order management machine, for example, reducing communication link amount of information more is also considered by coding this part and using the conversion table of a corresponding software name and a corresponding code. software B That is, with Software A, if it becomes and only the code of No. 2 and software B will become, it will be at the condition of the code of No. 10.

[0123] Moreover, although the exchange of the information between a software effector and an order management machine was explained as what human being performs through a telephone, it prepares both a transceiver machine and may be made to deliver and receive information in each above-mentioned example through a channel.

[0124]

[Effect of the Invention] According to invention of claim 1, a software effector generates the right of activation of software only by entering the right generation password of activation of the normal corresponding to an order. And the amount of information which should be sent can be reduced sharply, without degrading safety, since only the information which gives authorization for the right generation password of activation, i.e., a software effector, to generate the right of software activation corresponding to ordering information to a software effector is sent from an order management machine. Moreover, the amount of information of the right generation password of activation can always be realized for small amount of information, without being dependent on the number of the software to order. That is, even if a software effector places an order for two or more software at once, the amount of information becomes the same as the amount of information of a placing-an order for one software case. When transmitting and receiving a password especially by telephone by reduction of this amount of information, it is convenient in user interface. Moreover, for an order management machine, it tells and between **** decreases. Moreover, for the user of a software effector, in case it is heard wrong and this is inputted into an effector, between **** decreases. Moreover, since the time amount which has connected the telephone is also reducible, there is a merit also in tariff.

[0125] According to invention of claims 2, 5, 8, 10, and 15, since he is

trying to generate the right generation password of activation using a data compression function, the amount of information can be reduced further.

[0126] Since the right generation password of activation by which the digital signature was carried out to the software effector is sent according to invention of claim 3, it becomes almost impossible to forge the right generation password of activation by the software effector side, and a software protection system with very high safety can be realized.

[0127] According to invention of claim 4, the change value which changes whenever it creates ordering information is introduced. The right generation password of activation from an order management machine Since it is constituted so that it may become effective only with the software effector holding a corresponding change value, Even if it creates the same order as a different stage and enters the former right generation password of activation, the change value generated at the time of a next order differs from the change value generated at the time of a former order, and the entered password does not become effective. The injustice of repeating and using the right generation password of activation by it when a right of activation to which the count of activation is restricted is generated by this can be prevented.

[0128] Since the time stump currently held common to a software effector and an order management machine is used in order to distinguish sharply the order made at a different stage according to invention of claim 6, it is not necessary to send the information for sharp distinction to an order management machine from a software effector.

[0129] Since the order authentication information for which it depended on ordering information and effector confidential information by the software effector side is generated and he is trying to send to an order management machine according to invention of claim 7, in advance of issue of the right generation password of activation, authentication of ordering information and a software effector can be performed by the order management machine side. Since authentication of ordering information and a software effector is related to accounting in practice, it is an indispensable function. In this invention, this function is efficiently realized by notifying the order authentication information on a small digit count to an order and coincidence from a software effector. Moreover, order authentication information can be used also as order identification information which identifies an order.

[0130] Both a count limit function and a user authentication function can be realized without increasing the amount of the information

exchanged between a software effector and an order management machine according to invention of claim 9.

[0131] Since the right generation password of activation by which the digital signature was carried out to the software effector from the order management machine is sent according to invention of claim 12, it becomes almost impossible to forge the right generation password of activation by the software effector side, and a software protection system with very high safety can be realized.

[0132] The 1st right generation module of activation for activating the 2nd right generation module of activation stored in the software effector side according to invention of claim 13 is stored in an order management machine. Since this 1st right generation module of activation is included in the right generation password of activation and he is trying to send it, even if it is going to generate the right of activation unjustly, since it runs short in amount of information, by the software effector side, the right of right activation is ungenerable. Therefore, a much more safe software protection system is realizable.

[0133] According to invention of claim 17, since he is trying to eliminate the ordering information concerned after carrying out are recording maintenance of the created ordering information in un-volatilizing and generating the right of activation of corresponding software, a software effector can send only an order continuously for the time being, and can control activation of software based on the right generation password of activation returned behind.

[0134] According to invention of claim 18, since the hysteresis of the information exchanged mutually, respectively is held, a software effector and an order management machine can cope with the trouble produced behind flexibly.

[0135] According to invention of claim 19, the software effector and the order management machine hold the code corresponding to the combination of all software as a table, and since he is trying for a software effector to send the code obtained from the table to an order management machine as ordering information, it can reduce the amount of data of ordering information further.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the configuration of the software protection system concerning the 1st example of this invention.
[Drawing 2] It is the block diagram showing the configuration of the software protection system concerning the 2nd example of this invention.
[Drawing 3] It is the block diagram showing the configuration of the software protection system concerning the 3rd example of this invention.
[Drawing 4] It is the block diagram showing the configuration of the software protection system concerning the 4th example of this invention.
[Drawing 5] It is the block diagram showing the configuration of the software protection system concerning the 5th example of this invention.
[Drawing 6] It is the block diagram showing the configuration of the conventional software protection system.
[Description of Notations]
101-501 -- Software effector
102-502 -- Order management machine
3 -- Encryption software storing section
4 -- Order creation section
5 -- Effector ID storing section
6 -- Effector code key storing section
7, 21, 31, 43 -- Right generation password verification section of activation
8 -- Right generation section of activation
9 -- Right storing section of activation
10 -- Software decode activation section
11 -- Effector code key storing section
12, 22, 33, 47 -- Right generation password generation section of activation
20 -- Random-number generation section
30 -- Order authentication information generation section
32 -- Effector authentication section
40, 44, 50, 54 -- Order hash section
42 45 -- Exclusive-OR section
46 -- Effector authentication section
51 -- Right generation module of activation A storing section
52 55 -- Right generation password inverse transformation section of activation
53 -- Right generation module of activation B storing section
56 -- Right generation password generation section of activation